Testimony to the PEGA Committee
of the European Parliament

27 October 2022

The impact of spyware on fundamental rights

David Kaye*

Members of the PEGA Committee:

Thank you very much for the opportunity to appear before you today. I genuinely believe that this Committee can set the standard for the control of the kind of intrusive technologies on your agenda, and I thank you for taking on this work and rising to the occasion.

I am sharing along with this testimony an overview of key aspects of international human rights law applicable to spyware like Pegasus. I would also draw attention to the first and second footnote that identifies other work, including as the United Nations Special Rapporteur on freedom of opinion and expression from 2014 to 2020, that explores the human rights issues at stake and the policies that might address them.

In these introductory remarks, I would like to identify a series of related points that, in considering the fundamental rights at issue, bear the scrutiny of legislators and policymakers, especially but not only in Europe.

First, this Committee's remit focuses on the severe threats to freedom of expression, privacy, association and other fundamental rights posed by a particular type of aggressive surveillance tool. I understand that this is not *per se* about the NSO Group's Pegasus spyware, because we know that there is an opaque industry of spyware tools hidden from global attention right now. As such, my comments focus on the specific problems posed by intrusive spyware like Pegasus and not the broader but still serious problems of other forms of digital surveillance, mass and targeted.

Second, with the question of lawfulness in mind, what is it about this kind of spyware that requires urgent global action? I believe it is, in large measure, this: surveillance technologies like Pegasus give attackers an unprecedented power of intrusion and collection that fails to distinguish between legitimate and illegitimate targets of surveillance. It provides the attacker with the ability to gather and monitor its target's digital life without distinguishing, say, criminal conspiracy from an individual's opinions, communications, politics, contacts, location data, browsing habits, banking information, dining plans, and more, sometimes in real time. All of these human activities today are often mediated through our personal devices, for better or, as here, for worse.

* University of California, Irvine, School of Law; United Nations Special Rapporteur on Freedom of Opinion and Expression (2014 – 2022).

Third, given that extraordinary level of intrusion, the risks to fundamental rights are correspondingly severe. The rights at issue are not only those held by individuals as such. Yes, of course, human rights law – the International Covenant on Civil and Political Rights or the European Charter on Fundamental Rights or the European Convention on Human Rights – protects *individual* rights to privacy, opinion and expression. But these very rights are foundational to democratic societies, as the ECHR and Charter, and their case law, and the UN Human Rights Committee repeatedly make clear. Spyware causes individuals to doubt the privacy of their communications and opinions, strategically designed to cause people to question their intentions to engage in private and public discourse. I hardly need say this to legislators, but for democratic societies, that withdrawal can be fatal, particularly when the targets of such intrusions are those we depend upon to inform our public life and debate, such as human rights defenders, journalists, civil servants, and elected leaders like you.

Fourth, given the severity of the threats posed by such intrusiveness into individual life and democratic society, the burden to justify such threats falls on the attacker, here governments and the private actors that provide the tool. Put another way, human rights law places the obligation on the state to demonstrate that any burden it imposes on a fundamental right is justified by the law. It is emphatically not a matter of balancing interests but one of justifying a burden by legal standards. States and spyware companies argue that they need the tool in order to counter terrorism or other threats to national security and public order, but, as was clear in NSO Group's testimony in June, they are generally unwilling or unable to explain why that is so, how their tools meet basic human rights standards, always hiding behind state secrets, contractual arrangements and other excuses. These excuses, even if one thinks of them as legitimate, must nonetheless be supported by evidence. In its absence, the rule of law requires that we proceed on the assumption that such spyware fails to meet several key principles of international human rights law.

Fifth, the human rights to privacy and freedom of expression share a common, or close to common, set of standards that require the state to meet tests of legality, necessity and proportionality, and legitimacy. This means several things. It means that any burden on privacy or freedom of expression be provided or prescribed by law, precisely drafted to give the subject of regulation notice but also to limit the discretion of the state to impose any burden. It means that the restriction must be the least restrictive of available tools available to the state and that it impose no greater burden than necessary – and that the burden not eliminate the right entirely. And it means that the ends must be legitimate. These are cumulative standards; the attacker cannot simply say, for example, that the restriction is 'for national security.' They must demonstrate meeting each condition.

Sixth, every right must have a remedy for its violation. The ICCPR itself obligates states to ensure an "effective remedy". The nature of that remedy may exist along a spectrum, depending on the circumstances, from criminal accountability, restitution and compensation to satisfaction, apology, and guarantees of non-repetition. Unfortunately, too often states hide behind claims of sovereign immunity or national security to avoid liability and remedy. But impunity only incentivizes the use of the tool. However this Committee proceeds, remedy should be a part of the equation, consistent with human rights law.

Seventh, it is often suggested that human rights law applies only to states and not to private actors. This is not entirely true. For one thing, the state is obligated not only to promote fundamental rights, but also to protect the enjoyment of those rights. The state has an *obligation* to protect those within its jurisdiction against, for instance, interference with one's privacy, an obligation that should be understood to include transnational surveillance threats. But also, under the United Nations Guiding Principles on Business and Human Rights, adopted by the Human Rights Council over a decade ago, companies have a responsibility to prevent or mitigate human rights harms their activities cause or to which they contribute. The adoption of a human rights policy and an internal process to address human rights concerns is nice, even a prerequisite, but without transparency, external oversight, and remediation, it is window dressing, hardly even a first step.

Finally, in light of all that I have noted, I have serious doubts that surveillance technologies with similar characteristics as Pegasus can ever meet the tests of international human rights law. As such, their use should be considered unlawful. Your Committee's work, combined with actions such as the U.S. blacklisting of NSO Group, suggest that a ban of such technologies is the correct answer to result from your work.

At a minimum, however, I return to the call I made in 2019: the development, marketing, sale, transfer and use of tools like Pegasus should be brought under a moratorium – that is, temporarily halted – while states, regional institutions, and international organizations consider and implement a range of minimum steps that should be undertaken. Strict internationally agreed export control, genuine transparency and oversight, radical legal reform of surveillance practices and law, removal of barriers of sovereign immunity: these are a few of the steps that ought to be taken, again at a minimum, to begin the process of replacing a lawless use of technology with the rule of law.

Thank you very much.

Annex: Overview of the international human rights obligations applicable to the use of surveillance technologies

I. Executive Summary

1. This intervention provides the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware of the European Parliament (the Committee) with information and analysis concerning the impact of spyware on fundamental rights. As such, it focuses on individual rights and state obligations under international human rights law, in particular under the International Covenant on Civil and Political Rights ("ICCPR" or "Covenant"). It also addresses the responsibilities of private businesses. To a significant extent, this intervention draws upon my report to the Human Rights Council as United Nations (UN) Special Rapporteur on the subject of the private surveillance industry.[1] In the years since that report, I have continued to study, write, and testify concerning spyware's impact on human rights and legal and policy options available to governments and international organizations.[2]

2. All 27 Member States of the European Union have ratified the ICCPR, assuming the obligations imposed by the ICCPR to respect and ensure human rights.[3] This is, of course, in addition to Member State obligations under the EU Charter on Fundamental Rights and the European Convention on Human Rights. For the purposes of this intervention, and given the global reach of spyware tools such as Pegasus, I focus on and cite to articles of the ICCPR, which in this context imposes obligations quite similar, if not materially identical, to other fundamental rights obligations of EU Member States.

3. The actual and potential use of spyware interferes particularly with the right to privacy (Article 17), by undermining individuals' ability to "determine who holds information about them and how that information is used,"[4] and the rights to freedom of opinion and expression (Article 19), by causing an extreme and long-lasting chilling effect to a wide range of people, i.e., both actually and potentially targeted or to be targeted by spyware or those who meet or communicate with them such as their relatives,[5] lawyers,[6] and

---

[1] See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Surveillance and human rights (28 May 2019), A/HRC/41/35.
[2] See, e.g., David Kaye, *Here's what world leaders must do about spyware*, Committee to Protect Journalists (13 October 2022); David Kaye, *The Spyware State and the Prospects for Accountability*, 27 Global Governance 483 (2021); David Kaye and Marietje Schaake, *Global spyware such as Pegasus is a threat to democracy. Here's how to stop it*, The Washington Post (19 July 2021); and David Kaye, *The surveillance industry is assisting state suppression. It must be stopped*, The Guardian (26 November 2019). My testimony before the Indian Supreme Court technical committee addressing Pegasus allegations may be found at https://pegasus-india-investigation.in/depositions/prof-kaye-statement/ and https://cpb-us-e2.wpmucdn.com/sites.uci.edu/dist/2/4290/files/2022/02/Affidavit-David-Kaye-India-Supreme-Court-2021.pdf. My 2020 amicus filing in the United States Court of Appeals for the Ninth Circuit in *WhatsApp, Inc. v. NSO Group Technologies* may be found at https://freedex.org/wp-content/blogs.dir/2015/files/2020/12/Kaye-Amicus-Curiae.pdf.
[3] The Office of the High Commissioner for Human Rights (OHCHR), Status of Ratification Interactive Dashboard.
[4] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (17 April 2013), A/HRC/23/40, para. 22.
[5] See the testimony by Carles Puigdemont to the Committee (6 October 2022).
[6] See the testimony by Diana Riba i Giner to the Committee (6 October 2022).

journalistic sources.[7] Spyware also implicates other fundamental rights, such as the guarantees of peaceful assembly (Article 21) and association (Article 22) and the pervasive obligations of non-discrimination (Article 2(1), Article 4(1), and Article 26). It also may involve grave secondary impacts, implicating the right to life (Article 6), the prohibition of torture (Article 7), arbitrary detention (Article 9), and the right to freedom of movement (Article 12) and due process (Article 14). Among many sources, reports by organizations such as Citizen Lab, Amnesty International, Mexico's R3D and ARTICLE 19 have highlighted the various ways in which spyware has implicated these rights.

4. For the protection of human rights, the ICCPR imposes three sets of state obligations: (i) refrain from violating human rights;[8] (ii) prevent human rights interferences of third parties such as private actors or other states;[9] and (iii) provide remedies to victims of human rights violations.[10]

5. As a burden on fundamental rights to privacy and freedom of expression, any use of surveillance must meet the basic tests of legality, necessity, and proportionality, and legitimacy. Yet it is evident that the use of spyware with similar characteristics to the Pegasus malware likely does not meet the three-part test, raising grave concerns about its lawfulness as a general matter (that is to say, apart from its specific illicit uses). In particular, the use of Pegasus-like spyware may not satisfy the necessity and proportionality test as there is always a less restrictive alternative investigative method available to law enforcement or security service authorities. Further, it may be technically impossible for any state to implement sufficiently effective safeguards, which are required by the legality and proportionality tests, to eliminate the risk of spyware use which is not qualified as a permitted interference under these articles ("non-qualified use of spyware").

6. Even if one were to assume that there are extreme situations where the use of some forms of spyware could be qualified as permissible interference, a state should, at least:
    a. Exclude intrusive, mercenary spyware such as but not limited to Pegasus from any category of permissible surveillance technologies;
    b. Impose a moratorium on the use of spyware until it enacts law providing a narrow basis for the use of spyware and implements strict and effective safeguards;
    c. Impose a moratorium on the export of spyware until each state defines and implements sufficiently robust export controls; and
    d. Provide remedial pathways for victims, including lifting barriers to transnational litigation against responsible governments such as sovereign and official immunities.

---

[7] See the testimony by Stavros Malichudis to the Committee (8 September 2022). Mr. Malichudis, a Greek journalist, explained to the Committee that his journalistic sources, such as asylum seekers, had been already in a vulnerable situation but the use of spyware against him made them even more vulnerable, discouraging them to disclose information to him.
[8] Article 2(1) of the ICCPR.
[9] Article 2(1) of the ICCPR; Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant (26 May 2004), CCPR/C/21/Rev.1/Add.13, para. 8.
[10] Article 2(3) of the ICCPR.

7. I therefore urge the Committee to consider a ban of the use and export of spyware sharing the characteristics of Pegasus, and ensure the availability of remedies to individuals affected by spyware, in order to remediate the ongoing violations of the Covenants and ensure future compliance.

II. The actual and potential use of spyware interferes with the rights to privacy and freedom of opinion and expression of a wide range of individuals in a society.

8. Spyware directly implicates the rights to privacy, protected by the ICCPR Article 17, and to freedom of opinion and expression, protected by Article 19.

9. Article 17(1) guarantees that, as a basis of human dignity and integrity, "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence." "Privacy" includes informational privacy, namely, "the ability of individuals to determine who holds information about them and how that information is used."[11] The mere possibility of a spyware infection undermines an individual's ability to control their personal information and communication, thus interfering with their right to privacy.[12]

10. Article 19(1) guarantees the right to maintain opinions without interference, and as such, it permits no exception or restriction. Article 19(2) guarantees "the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers [...]." The right to freedom of expression is essential for both human dignity and democratic self-governance.[13] Spyware interferes with this right, as the actual and perceived imminent threat of retaliation incentivizes individuals to self-censor, prevents them from imparting their expressions and ideas, and deprives them of the ability to freely conduct research online or contact informational sources. Altogether, it prevents individuals from seeking and receiving information (such restriction is often referred to as a 'chilling effect').[14] In the digital age, the right to privacy is a gateway to the exercise of the right to freedom of expression because the lack of sufficient privacy protection leads to the chilling effect, which interferes with the right to freedom of expression.[15]

11. Journalists, human rights defenders, and politicians targeted by spyware have described their experiences for the Committee and other forums; however, it is important to

---

[11] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *supra* note 4.
[12] See Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (3 August 2018), A/HRC/39/29, para. 7, citing European Court of Human Rights, *Roman Zakharov v. Russia*, application No. 47143/06, judgment of 4 December 2015; and Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (30 June 2014), A/HRC/27/37, para. 20, citing European Court of Human Rights, *Weber and Saravia v. Germany* and *Malone v. UK*. See also, European Court of Human Rights, *Klass v. Germany*, para. 41.
[13] Human Rights Committee General Comment No. 34: Article19: Freedom of opinion and expression (12 September 2011), CCPR/C/GC/34, para.2.
[14] See Human Rights Committee General Comment No. 37 on the right of peaceful assembly (article 21) (17 September 2020), CCPR/C/GC/37, para. 10, 36, 61, and 94. See also, General Comment No. 34, *supra* note 13, para. 9 and 47.
[15] See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: The use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age (22 May 2015), A/HRC/29/32, paras.16-18.

understand that these victims have an exceptionally strong commitment to the common good in the society, and have overcome the significant chilling effects to go public. The chilling effect may impact a wide range of people. Due to the technical difficulties of confirming and attributing a spyware infection,[16] the chilling effects extend even to those who cannot confirm the actual infection but belong to a particular category of people against whom a government is motivated to surveil as well as any third party who may have imparted or received information from them.[17] Furthermore, the secrecy and technical particularities of spyware intrusions make it difficult for individuals to know of surveillance conducted against them. Thus, the knowledge or allegation of even one infected person creates a belief in broader surveillance, extending the possibility of chilling expression across a wide range of persons.

III. Spyware such as or equivalent to Pegasus fails basic requirements of human rights law.

12. The right to privacy and the right to freedom of expression allow for interference in exceptional cases where a state has shown that the prescribed conditions are met (Articles 17(1)(2) and Article 19(3)). Notably, the possibility of restriction does not pertain to the right to freedom of opinion.

13. Broadly speaking, both Articles require the application of the so-called three-part test (which require "legality," "legitimacy," and "necessity and proportionality"). Given the interlocking nature of both rights in the context of surveillance, all the distinctive elements in the tests under both Articles must be met.[18]

14. Legality means that the interference is provided by law, non-discriminatory, accessible, and specific enough to serve as an advance notice to individuals and as the limitation of a state's discretion;[19] and it is accompanied by strict safeguards which sufficiently eliminate the risk of non-qualified surveillance use are in place.[20]

    a. Legitimacy: State interest must strictly fall under one of the items in the exhaustive list in Article 19(3): rights or reputations of others; national security; public order; public health or morals.[21]

    b. Necessity and proportionality: The restriction must be: (i) appropriate to achieve the purpose; (ii) the least restrictive among options which might achieve the

---

[16] See Bill Marczak et. al., *The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit*, The Citizen Lab (20 December, 2020); Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 Harv. Int'l L.J 374, 399 (2011). See also, the testimony by Diana Riba i Giner, *supra* note 6.

[17] See Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (4 August 2022), A/HRC/51/17, para. 10 ("The mere existence of hacking programmes can have chilling effects on freedom of expression, the work of the media and public debate and participation, potentially eroding democratic governance").

[18] See Surveillance and human rights, *supra* note 1, para. 24.

[19] General Comment 34, *supra* note 13, paras. 24-27.

[20] See, id., paras. 23; Article 17(2) of the ICCPR; Human Rights Committee, *Madhewoo v Mauritius*, CCPR/C/131/D/3163/2018, paras. 7.4 and 7.6; Human Rights Committee, Concluding Observation on the United States of America (23 April 2014), CCPR/C/USA/CO/4, para. 22. See also The right to privacy in the digital age, (2014), *supra* note 12, paras. 28 and 37.

[21] General Comment 34, *su*pra note 13, paras. 29-32.

purpose and must not be overbroad; and (iii) proportionate to the interest to be protected in a specific situation.[22] The test requests "a detailed and evidence-based public justification."[23]

15. Applying the three-part test, a strong case can be made that the use of spyware with equivalent characteristics as Pegasus cannot satisfy the requirements of Article 17 and 19, for at least the following two reasons.

    a. First, spyware such as Pegasus allows indiscriminate and virtually (if not actually) complete access to data and recording functions on a target's device. Such access lacks discrimination, the ability to distinguish between, for instance, warranted and non-warranted information-access. Intrusive spyware does not separate information relevant to a legitimate investigation from information outside the investigation's scope.[24]

    b. Second, it is highly questionable whether safeguards that sufficiently eliminate the risk of non-qualified use of spyware are practically possible. Considering both the innate high risk of non-qualified spyware use demonstrated over the course of this Committee's work and the inherent limitations of checks and balances, such effective safeguards may be virtually impossible.

IV. State obligations to protect and promote human rights apply to spyware use, export and remedy.

16. Under the ICCPR, a state is obligated to: (i) refrain from violating the human rights protected by the ICCPR (Article 2(1)), (ii) prevent the violation of such rights by third parties such as other states and private individuals or entities (Article 2(1))[25], and (iii) provide remedy to individuals whose rights have been violated (Article 2(3)). Assuming that the use of spyware with characteristics of Pegasus violates Articles 17 and 19, states are obliged to perform the following three duties.

17. First, the state is obligated to refrain from the use of spyware. Further, states should pursue a global ban because of the technology's ability to infringe on the rights of individuals "regardless of frontiers."[26]

18. Second, given that Article 19(2) protects the right to seek, receive, and impart expression "regardless of frontiers," a state should prevent the use by domiciled companies of

---

[22] Id., paras. 33-36.
[23] The use of encryption and anonymity, *supra* note 15, para. 35.
[24] David Pegg and Sam Cutler, *What is Pegasus spyware and how does it hack phones?*, The Guardian (18 July 2021).
[25] General Comment No. 31, *supra* note 9, para. 8; Human Rights Committee General Comment No. 16 (1988):Article 17 (Right to Privacy), CCPR/C/GC/16, paras. 1 and 9; General Comment No. 34, *supra* note 13, para. 7.
[26] See the testimony by Carine Kanimba to the Committee (30 August 2022). See also, The right to privacy in the digital age (2022), *supra* note 17, para. 9 and note 16.

spyware outside its jurisdiction.[27] As such, the state has the duty to ban the export of spyware by vendors under its jurisdiction.[28]

19. Third, as a part of the duty to provide accessible and effective remedy to victims, states should establish appropriate judicial and administrative mechanisms for addressing claims of violations, investigate allegations of violations, provide reparation, and hold accountable the perpetrators of human rights violations.[29] Given the covertness of infection and the technical difficulties of confirming and attributing an infection, a state should provide ex-post notification to all individuals against whom spyware is used so that they can exercise the right to remedy.[30]

20. Further, foreign sovereign and official immunities should not apply to protect state or non-state actors responsible for targeting individuals with spyware across borders. This is in part because states have an obligation to take positive steps to protect the enjoyment of individual rights and remedies.[31]

21. Even if there were situations where non-Pegasus spyware use can be qualified as permitted interference, I would nonetheless recommend a number of actions to ensure that the state remains compliant with its human rights obligations.

22. First, as a part of the duty to refrain from human rights violations, a state should, *prior to using spyware*, enact law that constrains the state's use of spyware in order to meet all required elements under the legality test; and design and implement safeguards which are sufficiently effective to eradicate the risk of non-qualified use of spyware. The safeguards should include, at a minimum, independent and impartial judicial pre-authorization of *all* cases of spyware use, regardless of domestic or extraterritorial use.[32]

23. Judicial pre-authorization is not likely to be sufficiently effective by itself.[33] Thus at least the following mechanisms need to also be in place.
    a. Effective and independent oversight which (i) monitors every process of each spyware use, including judicial pre-authorization, actual spyware use, and

---

[27] See, e.g., The use of encryption and anonymity, *supra* note 15, para 25. See also, General Comment No. 31, *supra* note 9, para. 2 ("every State has a legal interest in the performance by every other State Party of its obligations [under the ICCPR]").
[28] See Human Rights Committee, Concluding Observations on Italy (1 May 2017), CCPR/C/ITA/CO/6, para. 37. See also, The right to privacy in the digital age (2018), *supra* note 12, para. 25.
[29] General Comment No. 31, *supra* note 9, para. 15.
[30] See, for example, Concluding Observations on Italy, *supra* note 28, para 37; Concluding Observations on Poland (23 November 2016), CCPR/C/POL/CO/7, paras. 39 and 40; Concluding Observations on Ukraine (9 February 2022), CCPR/C/UKR/CO/8, para.42. See also, The right to privacy in the digital age (2014), *supra* note 12, paras. 39-41.
[31] See note 27.
[32] See Concluding Observations on Italy, *supra* note 28, para. 37. See also, The right to privacy in the digital age (2018), *supra* note 12, para. 39 ([the judicial branch] "needs to make sure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary, and proportionate and authorize (or reject) ex ante the surveillance measures;" The right to privacy in the digital age (2014), *supra* note 12, para. 30.
[33] Panel 2 (Safeguards and Supervision) at the Committee hearing on 13 June 2022 discussed several limitations of judicial authorization, e.g., (i) independence and impartiality of judges are not always guaranteed; (ii) state agencies who wish to use spyware may deceive or hide critical information from judges when seeking pre-authorization, (iii) actual use of spyware may deviate from pre-authorization.

termination of the use, (ii) investigates alleged unqualified use of spyware, and (iii) publicly discloses the result of such oversight for public scrutiny;[34]

b. Prohibition of data sharing and data repurposing;[35]
c. Prohibition of use of evidence which is directly or indirectly obtained through the misuse of spyware.[36]

24. Given that it takes time and resources to complete these obligations, states should adopt a moratorium on spyware use in order to eliminate the risk of non-qualified use of spyware. States should make efforts to broaden such a moratorium at the global level.[37]

[34] See, for example, Human Rights Committee, Concluding Observations on Macao, China (27 July 2022), CCPR/C/CHN-MAC/CO/2, paras. 33; Human Rights Committee, Concluding Observations on Georgia (13 September 2022), CCPR/C/GEO/CO/5, para. 40. See also, The right to privacy in the digital age (2018), *supra* note 12, paras. 39 and 40; The right to privacy in the digital age (2014), *supra* note 12, para. 37 and 38.
[35] See *Madhewoo v Mauritius*, *supra* note 20, paras. 7.4 and 7.6; Concluding Observations on Canada (13 August 2015), CCPR/C/CAN/CO/6, "C. Counter-terrorism."
[36] See Human Rights Committee, General Comment No. 20: Article 7 (Prohibition of torture, or other cruel, inhumane or degrading treatment or punishment (10 March 1992), para. 12.
[37] So far, Costa Rica has joined the call for a moratorium. See Access Now, *Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology* (13 April 2022).